Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0419U005063

Особливі позначки: відкрита

Дата реєстрації: 04-12-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Рахма Мохаммед Кадім Рахма
2. Rahma Mohammed Kadhim Rahma

Кваліфікація:

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: кандидат наук

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 29-11-2019

Спеціальність за освітою: Комп'ютерні системи та мережі

Місце роботи здобувача: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. С. Бандери, 12, м. Львів, Львівська обл., 79013, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про дисертацію

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 35.052.08

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. С. Бандери, 12, м. Львів, Львівська обл., 79013, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. С. Бандери, 12, м. Львів, Львівська обл., 79013, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.51.35

Тема дисертації:

1. Моделі та методи побудови операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих

2. Models and methods for constructing operating units for Galois fields used in cryptographic data protection based on elliptic curves

Реферат:

1. Дисертацію присвячено вирішенню науково-прикладного завдання створення операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих. Основну увагу приділено розробці методів оцінювання часової, структурної та ємнісної складності помножувачів елементів розширених полів Галуа GF(dm), методу оцінювання складності злому апаратних засобів КЗІ та методу маскування їхньої роботи, а також вдосконаленню методу вбудованого тестування операційних вузлів. Оцінювання складності базується на представленні структури помножувачів у вигляді матриці модифікованих комірок Гілда, з первинним аналізом їхньої складності для різних полів і

врахуванням отриманих результатів при оцінюванні складності помножувачів. Застосування розроблених методів дозволило визначити найкращі в порівнянні з двійковими розширені поля Галуа (серед полів з приблизно однаковою кількістю елементів). Ними виявилися поля з характеристиками 3, 5 та 7. Також встановлено значно меншу структурну складність помножувачів для поліноміального базису в порівнянні з нормальним, що пояснює складності імплементації помножувачів для нормального базису в ПЛІС. Запропоновано і реалізовано метод маскування роботи інверторів. Вдосконалено метод вбудованого тестування помножувачів. Реалізовано засіб проєктування у вигляді генератора моделей помножувачів та інверторів, з його допомогою розроблено ряд помножувачів та інверторів, виконано перевіряння адекватності запропонованих методів та засобів, здійснено їхнє впровадження. Результати дисертаційної роботи впроваджено під час виконання проєктних робіт на ф. AL-NABAA Network Solution L.L.C. (Багдад, Ірак), при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» та в навчальному процесі Національного університету «Львівська політехніка».

2. The dissertation is devoted to the solution of the scientifically applied problem of creation of operating units for Galois fields used in cryptographic data protection on the basis of elliptic curves. The main attention is paid to the development of methods for estimating the time, structural and capacitance complexity of multipliers of elements of extended Galois fields GF(dm), the method of assessing the complexity of hacking hardware cryptographic data protection tools and the method of masking their work, as well as improving the method of embedded testing of the operating units. Complexity estimation is based on the representation of the multiplier structure in the form of a matrix of modified Guild cells, with an initial analysis of their complexity for different fields and taking into account the results obtained when evaluating the multiplier complexity. The application of the method: an extended Galois field is selected; the basis for representing the elements of the Galois fields is selected; the basic elements of the multiplier are selected; the structure of the basic elements is selected; the structure of the multiplier is selected; the selected type of complexity is analyzed, relative values of complexity parameters are formed with respect to similar parameters of the extended binary field; studies are repeated for all selected to analyze extended Galois fields; the results of the study are recorded; the best field is determined. The application of the developed methods allowed us to determine the best Galois extended fields in comparison with the binary ones (among fields with approximately the same number of elements). They were fields with characteristics 3, 5 and 7. A significantly lower structural complexity of multipliers for the polynomial basis than the normal one was also established, which explains the difficulty of implementing the multipliers for the normal basis in the FPGA. A method of masking the operation of inverters is proposed and implemented. The method of built-in multiplier testing is improved. Code combinations that will never be encountered when processing elements of an extended Galois field during normal operation of processor nodes, memory nodes, and data channels exist. These unused (forbidden) code combinations can be used to monitor the performance of data protection tools while performing their essential functions (built-in controls can be implemented). But 100% of all, even single, errors can not be detected. The results obtained should be considered as an estimate of the proportion of errors that can be detected by the proposed method. A table-based method for describing the occurrence of erroneous codes is suggested. The method of masking the operation of hardware units for finding inverted elements in extended binary Galois fields in a polynomial basis is presented. The development of a method of masking operating nodes for Galois fields used in data protection based on elliptic curves consists in equalizing the computation time of inverted elements in a polynomial basis by refusing to use the Euclid generalized algorithm in favor of direct binary algorithms or exponential algorithms. The use of exponential algorithms requires the efficient operation of squaring or finding the square root. Masking through the use of the proposed methods leads to an increase in the time of finding the inverted element and (or) to an increase in hardware costs. The structure of the special processor for processing elements of extended Galois fields is proposed. The design tool was implemented in the form of a generator of multiplier and inverter models, with its help a number of multipliers and inverters were developed, checks of adequacy of the proposed methods and means were carried out, their implementation was carried out. The results of the dissertation work are implemented during the execution of design works on f. AL-

NABAA Network Solution L.L.C. (Baghdad, Iraq), during the state budget research work of the DB/KIBER "Integration of methods and means of measuring, automation, processing and protection of information in the base of cyber-physical systems" and in the educational process in Lviv Polytechnic National University.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Глухов Валерій Сергійович
2. Hlukhov Valerii Serhiiovych

Кваліфікація: 05.13.05

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Потій Олександр Володимирович

2. Potii Oleksandr Volodymyrovych

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Николайчук Ярослав Миколайович
2. Nykolaichuk Yaroslav Mykolayovych

Кваліфікація: 05.13.05

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Стадник Богдан Іванович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Стадник Богдан Іванович
Відповідальний за підготовку облікових документів	

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.